UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

Civil Action No. 1:12-cv-00629

vs.

Dlott, J.
Bowman, M.J.

Awareness Technologies, Inc.
Defendant.

PLAINTIFF'S S THIRD MOTION FOR LEAVE TO FILE THIRD ENLARGED AMENDED OBJECTION TO REPORT AND RECOMMENDATION (DOC.#225); OR ALTERNATIVE RELIEF

Pursuant to Rule 72 of the Federal Rules of Civil Procedure, Plaintiff, Javier Luis, herein submits his motion for leave to file his amended objection to the Magistrate's report and recommendation ("RR") (Doc. # 225). Plaintiff also needed to refile because he had not motioned for leave to file an enlarged Objection for good cause shown, as follows:

This case involves the Federal Wiretap Act ("the Act") and its updated version, the Electronic Communications Protections Act ("ECPA") (together as "the Act" or "ECPA"). Together the statutes have been described as "a complex, often convoluted, area of the law"[1] and as "an evidentiary nightmare."[2] The ECPA governs an area of law whose interpretation by the

[1] *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998)
[2] *United States v. Councilman*, 245 F. Supp. 2d 319, 321 (D. Mass. 2003)(vacated en banc, 418 F.3d 67 (1st Cir. 2005).

court system over the years has led to the interaction between two of its statues to be described as, among other things, "one of the most complex, convoluted statutes ever to emerge from the sausage factory on Capitol Hil."[3] Scholar Orin Kerr has called it "famously complex, if not entirely impenetrable."[4] The ongoing ambiguity regarding the scope of the law in regards to "transmission" of electronic communications has been documented throughout the Courts of Appeals.[5] The Fifth Circuit has documented their frustrations with these statutes, having stated, that the Act was 'a fog of inclusions and exclusions' that frustrated the judicial search for 'lightning bolts of comprehension,'" and was "fraught with trip wires." *Id.*

Ironically, all of the above concerns a law that was passed to instill *confidence* in the public over the safety of its private communications over the Internet.[6] Nonetheless, the ECPA is not only ludicrously out of date, but it is also so notoriously misunderstood that legal experts routinely lament the "messy" state of electronic privacy law it has brought about.[7]."

As can be seen, no this is no ordinary arena of law. Therefore, due to the exceptional circumstances involved within this complex arena of law, the impressive length of the Magistrate Judge's report, the plethora of errors objected to, Plaintiff requests that this Court allow Plaintiff to file this enlarged objection.

Wherefore, for good cause shown, Plaintiff respectfully requests that this Court allow submission of this out of time enlarged Objection. In the minimum, Plaintiff believes he should

---

[3] Kurt Opsahl. *Definitions Matter: Why We Filed an Amicus Brief in Snow v. DirecTV*. October 5, 2005.
[4] Orin S. Kerr, *Lifting the 'Fog' of Internet Surveillance*: *How A Suppression Remedy Would Change Computer Crime Law*. Hastings Law Journal, 2003
[5] Kerr, *Suppression*, supra at note 5, at 820 (first quoting *Briggs v. Am. Air Filter Co.,* 630 F.2d 414, 415 (5th Cir. 1980), and then quoting *Forsyth v. Barr*, 19 F.3d 1527, 1542-43 (5th Cir. 1994)).
[6] *See, ex.* Testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology to the House Committee on the Judiciary Subcommittee on Courts and Intellectual Property. March 26, 1998. *Available at* https://cdt.org/insight/testimony-of-deirdre-mulligan/
[7] Julian Sanchez, Internet Privacy Law Needs an Upgrade. CATO Institute. March 31, 2010.

be allowed to submit an equal number of pages as were contained within the report. In the alternative, if such relief cannot be granted, that this Court allows into the record the portions of this attached Objection that it sees fit to accept above the normal page limits. [8]

Dated: May 15, 2018

Respectfully Submitted,
/s/ Javier Luis, Pro Se
jdluis65ohio@gmail.com

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Objection was filed electronically on May 15, 2018. Parties may access this document through that system.

/s/ Javier Luis, *Pro Se*

[8] Only an hour after Plaintiff sent in his amended objection on Monday May 7 (Doc #232), the clerk's office sent a "Notice of Correction re:[231]." Plaintiff only recently found out about the notice due to an issue with re-installed software that has caused a few problems with the email desktop client and that is also causing anything from CMEC to be saved as an inoperable HTML instead of pdf as it had previously done. Regardless, the notice indicated Plaintiff needed to refile the document, which he did 5/11 (Doc.#233). However, Plaintiff had asked for an extension of time the previous week, but the request had not been ruled on. The coincidental timing of the notice after Plaintiff's submission of Doc.# 232 seemed to imply that the request was not granted, since had it been, then that day's filing which the clerk likely did see would have made the need to replace #231 moot.. That would cause the Court to have to consider two objections. To fix that, Plaintiff sent in Doc 233 which was meant to aid judicial economy, having roughly combined 231 and 232 into one document (233) which was just barely filed within the requested extension of time. In order to address that and aid in judicial economy as well as making this submission easier to read for the Court, Plaintiff requests that this out of time enlarged submission be granted so that the Court need only consider one Objection. Plaintiff is uncertain as to how to properly phrase that according to local rules.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

Civil Action No. 1:12-cv-00629

vs.

Dlott, J.
Bowman, M.J.

Awareness Technologies, Inc.
Defendant.

PLAINTIFF'S AMENDED OBJECTIONS TO MAGISTRATE'S REPORT AND RECOMMENDATION

Plaintiff objects to all of the Magistrate Court's (or "MC') rulings in the Report and Recommendations ("RR"), believing the case law and reasoning used led to an improper conclusion an absurd legal result. Plaintiff believes the findings in the RR wrongly opposes congressional intent in its construing of the Wiretap Act ("the Act" or "ECPA"), and runs afoul of technical realities related to computer hardware and the delivery mechanisms running the internet. Also the MC's findings run counter to more more technically and constitutionally sound judicial interpretations of what comprises an "intercept." Perhaps most unfortunate of all, the RR is also dangerously counter to our already battered privacy interests in this ever-changing Digital Age.[1]

[1] This issues herein have been argued many times in the five years the case has been in this forum. Although plaintiff again incorporates those arguments by reference, it is perhaps wise to also *directly* reference and re-argued those points herein. As such, many of these arguments will cite to plaintiff's own previously submitted documents containing those arguments–both in this forum and in his prior appeal.

Introduction

Much to its credit, a few years ago the Magistrate Court (or "MC") impressively rejected decades of improper reasoning as to a critical issue within the Wiretap Act, while suggesting that "a rethinking of the definition of the 'contemporaneous' standard of intercept might be necessary and that the timing of the intercepted data's transmission should be irrelevant, allowing the ECPA to be applied." Gariella E. Bensur, *Cover your Webcam: e ECPA's Lack of Protection against Software That Could Be Watching You*, 100 Cornell L. Rev. 1191 (2015)[2] Apparently, a "rethinking" of the contemporaneous standard did happen in the lower forum. However, the MC's new ruling is now completely opposite the advanced approach the Court strongly advocated in 2013 in a way that is not well explained by the Appellate Court's adoption of the contemporaneous standard, nor by the different standards applied to this summary judgment stage of this lawsuit. The Magistrate Court has sided with circuits that have (plaintiff believes) neutered the ECPA's intended protections due to the effective removal of privacy containing transient temporary storage that is more properly classified as memory than it is storage) which is necessary to the transmission of data from the type of communications the Wiretap Act was meant to protect. No matter, the Magistrate Court got it right the first time around and so the District Court should reject the recent RR in its entirety.[3] This Objection advocates for the correct application of Congress' intentions when it authored the Wiretap Act, which runs parallel (and should simultaneously serve) to Plaintiff's objections of the errors made by the Magistrate Court which has once again utilized

[2] referring to *Luis v. Zang*, No. 1:11-cv-884, 2013 WL 811816 at *6–7 (S.D. Ohio Mar. 5, 2013). Available at: http://scholarship.law.cornell.edu/clr/vol100/iss5/4

[3] Many courts apparently disfavor such wide-scale use of argument incorporation. Nonetheless, Plaintiff incorporates all relevant arguments made during this case. Most of those are located within six particular documents in the lower forum (Doc. #'s 91, 97, 118 and 222 in the 629 case and Doc. #'s 101 and 175 in the 884 case) and those argued in appeals (Document # 7, 13, 26, 35 and 43). While all the earlier arguments are adopted by reference herein, they will be re-argued here again as a precaution. Any relevant arguments mistakenly omitted should nonetheless be considered already argued and properly objected to for appeals.

improper reasoning and myopic vision in reaching a conclusion that undermines our privacy rights in the digital age and represents an absurd result.

Standard of Review

When reviewing a Magistrate Judge's report, a District Judge reviews *"de novo* any part of the magistrate judge's disposition that has been properly objected to." Fed. R. Civ. P. 72(b); *see also* 28 U.S.C. § 636(b). The District Judge has discretion to "accept, reject, or modify" the recommended disposition made by the magistrate judge. Fed. R. Civ. P. 72(b); 28 U.S.C. § 636(b). Although the district judge may also review de novo any portion of the magistrate judge's report that a party did not object to, the court is under no obligation to do so. Un-objected to portions of the report considered by the district judge will ordinarily be reviewed under the stricter plain error or manifest injustice standard

ARGUMENT

I. The Magistrate Court Erred Throughout Its Report and Throughout This Entire Case

Plaintiff believes the Magistrate Court erred in at least the following ways within its RR; (1) by using the wrong, outdated and narrowest approach to the contemporaneous standard while having placed too much weight on Tech's CEO's affidavit. That incorrect approach effectively terminated portions of the case affected by the issue of "intercept," but the MC also improperly negated portions dealing with section 2512 that other courts have found not be dependent on intercept as long as there has been actual acquisition in the presence of other factors that are present here - such as Tech's disclosure and use. Moreover, state and civil should have remained intact and unaffected regardless of that error. This lawsuit could move forward as to those issues regardless of whether or not that the intercept portion (and that affected by that ruling)are

invalidated by this Court or the Appellate Court[4] , and (2) because all of Plaintiff's claims were dismissed, the MC should have declined to exercise supplemental jurisdiction over Appellant's state and common law claims; among them the Ohio Wiretap claims, as well as Plaintiff's breach of privacy claims and intrusion upon seclusion,[5] and (3) by refusing to consider amended documents prior to issuance of her RR that pointed out specific facts in evidence that present issues at trial, and (4) by not recognizing that even without acceptance of the amendments, there is evidence in the record that Awareness acquired, disclosed, and intentionally used Plaintiffs Electronic Communications having reason to know they were illegally obtained , (5) with its tentative suggestion/partial recommendation that plaintiff might lack lack standing to bring an invasion of privacy claim under Ohio Law, and (6) by finding that Awareness is

[4] Note that Plaintiff is not necessarily advocating for the newly adopted standard to be abandoned entirely. However, for this case to head to trial, the contemporaneous standard itself would not have to be invalidated, only the MC's narrowest approach to that standard. The Sixth Circuit adopted the standard, but it did not clearly define its intended approach to the standard as did the Court in *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) and other similar rulings. Plaintiff believes this circuit should mimic that more modern, advanced and technically proper approach evidenced in *Councilman* where the Court found that the text of the statute does not specify whether the term "electronic communication" includes communications in electronic storage, but that the legislative history of the ECPA indicates that Congress intended the term to be defined broadly. Furthermore, that history confirms that Congress did not intend, by including electronic storage within the definition of wire communications, to thereby exclude electronic storage from the definition of electronic communications." Timothy J. Miano, *Formalist Statutory Construction and the Doctrine of Fair Warning: An Examination of United States v. Councilman*."

[5] *RWJ Management Co., Inc. v. BP Products North America, Inc*., 672 F.3d 476, 479 (7th Cir.2012) (there is a "presumption" that the District Court will decline to exercise supplemental jurisdiction if it has dismissed all federal claims before trial); see also 28 U.S.C. § 1367(c)(3). Evaluating considerations of judicial efficiency and duplication of judicial effort is not just a matter of toting up months or motions or the page counts of judicial orders. Rather, concerns about judicial economy have their greatest force when significant federal judicial resources have already been expended to decide the state claims, or when there is no doubt about how those claims should be decided." I*d.* At * 481 (citations omitted). Relinquishment will not lead to a "duplication of effort by a state court" if this the remainder of the claims are sent down because this Court has yet to rule on the merits, let alone on any issue of substance in this matter. Circuit courts haves upheld district court orders relinquishing supplemental claims that were much further along than this. *See, e.g., id*. (upholding remand of supplemental claims "just two business days before the two-week trial was scheduled to commence"); *Olive Can Co., Inc. v. Martin,* 906 F.2d 1147, 1153 (7th Cir. 1990) (relinquishing supplemental claims "just before trial after five years of discovery"). Judicial economy, therefore, does not weigh in favor of retaining supplemental jurisdiction.

entitled to Judgment on the §2511 claims based upon the lack of any 'intercept' of his 'electronic communications' while still 'in flight,' based in part by (a) the MC's improper interpretation of terms within the contemporaneous standard and (b) its ignoring the fact that the definition of "in flight" and "intercept" are not clear or universally defined by the circuit courts, and (c) its refusal to recognize that volatile/temporary memory is not the "permanent storage" intended to apply to the SCA instead of the Act, and (d) ignoring the fact that all parts of a communication- including what is found in the RAM- was also meant to be protected by the Act, and (7) by overlooking the critical importance of the type of acquisition involved in this case; i.e. continuous surveillance by automatic routing software, and (8) attaching no relevance to the undisputed fact that Tech engaged in the violation during a protracted period of time, and (9) with its ruling that Tech is entitled to judgment on the Ohio Wiretap Law Claim, and (10) ruling that Tech is entitled to judgment on breach of privacy claim, having partially based her reasoning on irrelevant matters having to do with (a) the licensing agreement, (b) the lack of evidence that the intrusion was "wrongful," or perhaps not wrongful enough to satisfy state standards (c) the allegedly private subject matter of the intrusion, having apparently found the messages were not so private as to deserve extra protection (and (d) with its findings about Plaintiff's supposed lowered expectations of privacy due to its incomplete and erroneous findings that married people have a lowered expectation of privacy within their digital world, and (11) by its continued use of cases that have little to nothing to do with the unique circumstances in this case, and that indeed sometimes support this case more than help defeat it.

A. Critical issues of fact remain unexplored or answered

Finding that there is no dispute as to the question of whether Tech's device intercepts contemporaneously due to the fact that Tech claimed WebWatcher copies the information from

the computers RAM, the MC has ruled that if there is no "intercept" as described in the Act, there can be no other possible claims.[6] First Plaintiff does not believe Tech has has submitted either to Plaintiff during discovery or to this Court anything that clearly demonstrates that the actual functionalities of Web Watcher do not include a contemporaneous acquisition of still in transit electronic communications since Tech remains mysterious about the exact *timing* of its acquisition from RAM and forwarding to its own servers; a question Tech surely wants to stay away from. The MC apparently believed Plaintiff had no dispute because he agreed with Tech's summary of the case, although the MC ignored that plaintiff was only agreeing to the facts of the case as they were described in detail by Tech in its motion for summary judgment, not with anything else. While the timing of Tech's copying and subsequent acquisition seems to have been assumed a question of law, it seems more appropriate that the question of timing and acquisition be put before a jury.[7]

[6] While this Court could go against its Magistrate Court and adopt similar parameters within the contemporaneous standard as seen in other circuits, it is more likely that, in truth, this case has been effectively grounded until the question of whether or not this circuit will follow the old school circuits, or follow the more recent decisions found in the First and Seventh and consider that section 2511 has been triggered has to be answered on plaintiff's second trip to appeals. Preferably it would have been answered along with the rest of them during the first trip, and there likely must be a third. Nonetheless, one must preserve issues for appeals However, at least some important questions can be explored here.

[7] For example, at trial Webwatcher could be found to copy the information prior to RAM in some other internet facing or internet involved component of the computer wherein the communications can more readily be considered "in transit" since it has not reached RAM yet. Or jurors may find that copying from RAM is not copying form storage, since RAM is considered memory not permanent storage, which would change the variables. A jury needs to see and and decide for itself many of these questions of fact. Does acquisition prior to RAM memory storage count as contemporaneous? Is there such a possibility? Has Tech answered those questions? Plaintiff did not but he has not the expertise or access to them, but would have for trial. Also, does copying from RAM necessarily mean the intercept can not be contemporaneous? When it comes to email, maybe. But when it comes to instant messages, that's less of an open and shut case. This may be true for Wiretap Act related claims, but not so for a few of Plaintiff's other claims. However, the MC has based her ruling on past cases that dealt mostly with emails, without once considering that there is a fundamental difference between emails and the kind of communications primarily acquired by Tech in this case; Instant Messages. That question is not as simple as it seems and it involves almost no questions of law, but countless questions of fact that only a jury can decide.

There remain other § 2512 questions that some courts have ruled to be actionable even sans any actual "intercept" per se, as long as there there is actual acquisition, disclosure or use of the acquired communications, as noted below;

> The essence of our holding is that a defendant who manufactures, markets, and sells a wiretapping device in violation of 18 U.S.C. § 2512 is potentially liable in a private suit brought under § 2520 when that defendant also plays an active role in the operation of the device to "intercept, disclose, or intentionally use" a plaintiff's electronic communications. Put differently, the active operation of the device establishes that a defendant who has manufactured, marketed, and sold the device at issue (in violation of § 2512) has in fact participated in the intercept, disclosure, or use of a plaintiff's communications to such a degree that the defendant has "engaged in" the underlying violation. Manufacturing, marketing, and selling the device is thus a necessary prerequisite for a civil suit for a violation of § 2512; and, when that prerequisite is combined with the defendant's active operation of the device at issue, the defendant's conduct suffices to satisfy the "engaged in" standard of § 2520.
>
> –*Id.* at 27, 28

While Tech did object to its participation in any interception, that is not the only variable here. If it were there would be an "and" and not an "or" in the statue describing "intercept, disclose, or intentionally use." Tech never objected to or raised any questions as to its active participation in the operation of the device, nor did it bother to pretend it did not disclose or intentionally use those communications. Only during appeals did Tech seem to imply – but not actually argue – that it somehow had nothing to do with the marketing materials. Regardless, Tech's strategy was checked by Plaintiff's counsel which pointed out two more unanswered questions of fact when stating the following;

> Awareness cursorily disputes the validity of these exhibits for the first time on appeal … As a threshold matter, because Awareness did not challenge the validity of these exhibits below, it cannot do so on appeal…Because Awareness provides no argument to support its perfunctory assertion that "the validity of those documents are [sic] challenged" the issue is waived again…Awareness's implied arguments that these advertisements were not paid for or sponsored by Tech, at most create questions of fact. … Concerning Tech's previous affidavit, the Magistrate Judge correctly found that Mr. Miller's affidavit "is wholly silent regarding when WebWatcher forwards the recorded information to the secret account) Again Plaintiff's representatives correctly replied, "Awareness did not object to this finding…. Accordingly,

> Awareness has waived its ability to challenge this finding on appeal." (internal citations omitted)
>
> – Luis v. Zang, No.14-3601, Appelants Brief at 2,3

Similarly, in this lower forum, nothing Tech has submitted either to Plaintiff during discovery or to this Court clearly demonstrates that the actual functionalities of Web Watcher do not include a contemporaneous acquisition of still in transit electronic communications since Tech remains mysterious about the exact *timing* of its acquisition from RAM and forwarding to its own servers; a question Tech surely wants to stay away from. While this may be a question of law, it seems more appropriate that the question of acquisition be put before a jury. For example Webwatcher could at trial be found to copy the information prior to RAM, or a jury might find that RAM is more properly considered memory and not storage, which would change the variables. A jury needs to see and and decide for itself many of these questions of fact.[8]

B . Mc Erred With Its Improper Rejection Of Plaintiffs Amendments Which Pointed To Remaning Questions Of Fact

In plaintiff's attempted sur-reply which the MC rejected for no good reasons as it was submitted prior to her ruling, and should have been incorporated into her decision. In that sur-reply Plaintiff pointed out that issues of fact remained. The Sur-reply should have been considered by the MC which instead pointed out that it was only going to take into account

[8] Contrary to what the MC has asserted, Plaintiff never agreed with Tech on that issue, since he cannot truly know. This remains a question of fact. The MC declined to look at Plaintiff's submitted documents (Docs.# 222 and 223)- and this Court has yet to rule on Plaintiff's objection over the MC's refusal to admit those documents into the record during her exploration of her most recent report and recommendation. Luckily, the District Court can see it now, and judge for itself during its *de-novo* review, where Plaintiff believes new or lost or overlooked information by the MC is allowed into the record. As such Plaintiff proceeds herein on the assumption that this remains a question of fact, which then enables the rest of the appeal over the other issues, whether right or wrong.

Plaintiff's initial reply (Doc. #219) wherein plaintiff had mistakenly left out the remaining facts that should be allowed to be tried by a jury.

Among remaining facts that need to be tried by a jury is the following, as submitted in Plaintiff's Objection (Doc.# 224) and second motion for reconsideration (Doc. # 227). The filed motions, whether technically filed correctly or not should be considered part of the record as they were filed in the belief that the Court wanted them filed correctly. The Magistrate Court stated it was not charged with digging through the record to find previously submitted evidence. (Doc. # 224, pg. 5) Nonetheless, the Court is required to consider all previously submitted evidence evidence in support, in direct opposition, and all evidence properly before the court, including pleadings, depositions, answers to interrogatories, admissions, affidavits, transcripts, and written stipulations of fact. As such the rejected sur-reply should also have been considered part of the record as Plaintiff went through a lot of work to submit it.[9]

Moreover, as the MC noted in RR1, Plaintiff also alleged that Tech's "software did more than merely record keystrokes because it also saves and/or records entire IM conversations and other 'screen' data. A portion of the recorded data originated from Plaintiff, from a remote computer on which WebWatcher was (presumably) not installed. The affidavit submitted by the CEO confirms that much broader data than keystrokes is captured by the spyware at issue." *Id.* Thus, Tech's own CEO confirmed that – like most similar rootkit based software - Webwatcher also takes screenshots at certain intervals. That *confessed* (or at least strongly implied) functionality alone adds to the remaining questions in this case and that extra ability has often

[9] Among other things, it was intended to address the new claims by the CEO in the later filed affidavit that his company did not advertise those ads, nor did the ads point to the product purchased; the answer to which can be critical for section 2512 claims which do not live or die from 2511 alone. In its affidavit Tech's CEO claimed that the advertisements previously submitted were not advertising the WebWatcher system purchased by the main culprit, Joseph Zang, and that Tech had not marketed WebWatcher in the way it has previously seemingly accepted throughout this case.

been the difference maker in past decisions as to whether or not an "interception" has occurred in a case. While Webwatcher was not on Plaintiff's computer and thus not taking screenshots of his computer screen, it was taking screenshots on Catherine's screen (or it had the ability to do so) which was also displaying Plaintiff's private conversations in the opened IMs. The ability to take screenshots alone qualifies the mechanism as being capable of producing prohibited interceptions even under an interpretation of the FWA that requires interceptions of electronic communications to be contemporaneous with transmission. *See ex. Shefts v. Petrakis*, No. 10-CV-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012) (finding that software that caused images of the plaintiff's email communications to be captured as they were being written and sent or received "contemporaneously captured Plaintiff's electronic communications within the meaning of the [FWA]"); *see also Potter*, 2007 WL 539534, at *6 (holding that "incoming emails subjected to the screen shot software" satisfy the FWA's definition of an interception of an electronic communication).[10] Moreover, any remaining dispute as to how WebWatcher works is a question of fact that the MC now seems to be feel has been resolved. With what evidence, Plaintiff remains unsure.

Significantly, acquisition of AP's communications was never even *challenged* by Tech as there was plenty of evidence available to prove it had done so. Thus, arguing arguendo, even if *somehow* Tech was properly found innocent of liability for the *intercepts*,[11] Tech's "use" and

[10] Tech violated the FWA's prohibition on using unlawfully intercepted electronic communications when it summarized his private messages when they acquired them on their servers . See 18 U.S.C. § 2511(1)(d). Tech also violated the FWA's disclosure provision by having sent them via email to Joseph Zang. See 18 U.S.C. § 2511(1)(c*); see also Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009) (holding that 18 U.S.C. § 2511(1)(c) "protects against the dissemination of private communications that have been unlawfully intercepted").

[11] An Intercept (§2511) was previously found to have occurred, and when it was the MC did not use any lax filing standards to get to that conclusion/recommendation. Rather it was a well reasoned and thought out exercise free of any standards outside of the right path to pursue in order to fulfill Congress; intentions when it authored the Act and then later updated it in the ECPA. The findings did not rely on any inferences or fact that are not present now. The messages were not acquired any quicker then. In its exploration, the MC even noted that whether it was instantaneous or within a blink of an eye, the proper standard was well reflected by the *Klumb* case. The MC dismissed thee case, but not because of this issue, which was ruled Plaintiff's way. Having been sent back, this ruling should have remained the same. Even if Tech acquires the communications from RAM, the millisecond's difference should not have caused such an improper and abrupt about-face by the MC. Tech's

"disclosure" clearly violated the Act because Tech did not challenge or address AP's claims (in the lower proceedings or in appeals concerning the following; 1) its advertising for illegal use was illegal, and 2) that they *knew or should have known* the illegal nature of the communications it was acquiring, using and disclosing. Therefore, Tech's summaries and deliveries given its undisputed ability (and/or duty) to know the illegal nature of the intercepts is a clear violation of 18 U.S.C §§2511(1)(c), (d).[12] This presents a problem for the SD because it never discussed whether Tech "knew or should have known" that the communications were being illegally acquired on its servers.[13]

Another primary question of fact that remains is whether or not a jury would find that acquisition of data from RAM occurs fast enough to be considered "real time" and other similar questions having to do with the terminal intended terminal end point of a communication of an instant message versus that of an email. The answer of which can change the acceptance of "in flight" and when a message "comes to rest".

C. Tech and the MC relied upon irrelevant or distinguishable case law that interprets a previous version of the Wiretap Act, which has since been amended.

For better or worse, the contemporaneous requirement is, for now, the accepted standard within this Circuit. What matters most now is whether this Circuit will adopt the (plaintiff argues) outdated and "always technically wrong" narrow interpretation of that already overly

---

actual acquisition of Plaintiff's messages violation alone, with or without liability later attaching, would have been enough for the purposes of enabling standing to sue under §2512, as it was a violation of §2511. Most courts recognize a cause of action for §2512 when in the presence of any violations of §2511.

[12] Throughout these proceedings, Tech never one denied nor did it address AP's claims that it knew or should have known the illegal nature of the intercepts it was acquiring, using and disclosing.

[13] In the first half of this case, only by having *somewhere* explored or denied that Tech could not have known the illegality of the communications–an impossibility given Tech's advanced capabilities and infrastructure – could the SD have properly found that Tech's use and delivery did not violate §2511, thereby negating reach of remedies for violation of §2512. Instead, the MC looked towards other variables not considered relevant to liability under the Act.

narrow standard as adopted by the 3rd, 5th, 11th circuits – ancient and outdated rulings that were never technically correct, but that somehow have been adopted by the MC after it impressively rejected those approaches in its previous Report and Recommendation from 2013 ("RR1") (Doc. # 109 at p.*14) - or whether it will adopt the various broader approaches embraced by many state wiretap acts, some district courts within this same circuit, and sometimes evidenced within the appeals courts within the 1st, 7th, and 9th circuits; holistic legal approaches which plaintiff believes are much more enlightened as well as being constitutionally sound and technically proper. Moreover, none of those courts have rejected the "contemporaneous standard," and in fact, the First Circuit has specifically accepted the contemporaneous standard but from a broader perspective than what has been evidenced in this case and in those technically improper and outdated decisions within the (mostly) southern circuits.[14]

This Circuit can have its cake and eat it too. As shown by the First Circuit's ruling in *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(en banc), within that controversial contemporaneous standard lies some space for interpretation that allows a circuit to both accept the contemporaneous standard, and yet allow for a broader more enlightened approach that would allow for this case to proceed to trial ; one similar to the approach this same Court advocated so eloquently in 2013.[15]

---

[14] Plaintiff has previously stated (and recent world events have only confirmed) that the most backwards and despicable judicial decisions seem to emanate from the bowels of the country; aka the South (regarding the Act, such embarrassing, unconstitutional and technically flawed decisions as *Turk, Steve Jackson, Steiger, Simpson*). Its as if "Anti-lectuals" like Trump nominated everyone in those circuits. This is still a battle of North versus South in a way. It may always be that way. The Sixth should not follow those backwards circuits into the dystopian rabbit hole they want to drag us down into. The North is our only hope.

[15] The differences between the circuits are critical distinctions that can help mold our digital privacy protections for many years to come. While the District Court is perhaps not a forum that can by itself change the operating standard in this circuit, it could nonetheless advocate the more sophisticated and technically correct approach with its rejection of the MC's oddly new regressive approach to a matter it had once advocated rather well. To help reach that decision, this Court should reconsider the plethora of outdated circuit decisions that the 3rd, 5th, and 11th have used as the foundation for their contemporaneous arguments; one that requires a different treatment of electronic communications/emails in storage than those in transit. As previously discussed, that distinction is not supported by the Act nor is it found within its plain language. Congress never excluded electronically stored information from electronic communications, but it did from wire and oral communications.

D. The MC Ignored fact that WebWatcher is a type of automatic routing software and by Ignoring the Type of Acquisition Involved in this case and that Tech engaged in the violations during a protracted period of intercept.

As properly explored in Councilman, the use of automatic routing software is a game changer when deciding whether or not an "intercept" occurred under the Wiretap Act.

> [U]nder the narrow reading of the Wiretap Act we adopt ., very few seizures of electronic communications from computers will constitute 'interceptions.' . 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-Mail within the prohibition of [the Wiretap Act] is virtually impossible.'

– US v. Councilman, 373 F. 3d 197 (1st Circuit 2004)

Even if the narrowest interpretation of "interception" was properly used by the MC (which plaintiff believes it *was not*) the MC's ruling remains flawed if only because of the type of acquisition evidenced in this case. In a somewhat similar case*, Blumofe v. Pharmatrak, Inc*., 329 F.3d 9 (1st Cir. 2003), the court noted that the concept of a contemporaneity or real-time requirement, which evolved in other factual contexts, may not be apt to address issues involving the application of the Wiretap Act to electronic communications. *Id*. at * 21-22. The court also found that interception would be justified even under the contemporaneous standard of intercept when a program automatically duplicated part of the communication between a user and intended recipient and sent the information to a third party. *Id.* Cases such as *Pharmatrak* still support this case even under the narrowest definition of intercept available. In this case, Tech's software, *Webwatcher*, acted much like a data logging program, but after the data was recorded, it then *also acted* as an automatic routing program since the user never had to do anything to

send the acquired information to Awareness Tech's private servers thousands of miles away. So the program *itself* automatically sent the information.

> We then noted that Pharmatrak's program would qualify under the *Steiger* definition because it effectively was an automatic routing program. Id. Much like the data logging program there, the Procmail recipe file here acted as an automatic routing program. It analyzed all of the e-mails sent to Councilman's mail server in real time and copied the relevant ones while they were being delivered.
> – *US v. Councilman*, 373 F. 3d 197 (1st Circuit 2004)

Thus, the acquisition of Plaintiff's data, in this case, mimics that found in *Pharmatrak* and the software used also automatically re-routed the acquired information. Therefore, the reasoning used by the Court in *Councilman* should be instructive to this Court as it surely will be to the appellate court in the coming appeal. Therefore, whether right or wrong about its acceptance of the narrowest reading of the already destructively narrow contemporaneous standard, Plaintiff retains standing because, as the Court in *Councilman* stated, "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." *Id.* at 215.

Even more than emails, instant messages (IMs) reveal the weaknesses of the storage-transit dichotomy because IMs are "seldom saved" on the computer used to send or receive them, instead residing on a provider's internet servers. (R. 39, Compl. Pl.'s Ex. D2, PageID # 351.) IMs are not typically transmitted intact over dedicated circuits, but, like emails, are broken into "packets," sent over a network, and reassembled by the recipient's computer. *See Szymuszkiewicz,* 622 F.3d at 704–05; *Councilman*, 418 F. 3d at 69–70. Thus, when WebWatcher acquires IMs "in REAL TIME," as it claims on thousands of ads on the internet and has admitted to in this case, it acquires them in transient electronic storage. Electronic communications acquired while in transient electronic storage are intercepted contemporaneously with transmission because such storage is "part of the overall transmission process of an electronic

message." *In re Carrier IQ*, 78 F.Supp. 3d at 1081. In *In re Carrier IQ*, plaintiffs challenged software on mobile devices that "surreptitiously intercepted personal data and communications and transmitted this data to Carrier IQ and its customers." *Id.* at 1058. The court drew a distinction between acquisitions of communications that "occurred after the transmission was completed" and the case before it, where the challenged software was "alleged to operate on sent and received communications during the transmission process." *Id*. at 1078. The court found that, even if text messages "were in transitory storage on Plaintiff's mobile devices," the software could still intercept them "contemporaneous with their transmission." *Id*. at 1081. "[T]o hold otherwise would make the Wiretap Act turn on the intricacies of a particular circuitry's design: e.g. whether there is cache memory—an engineering intricacy that has no evident relationship to the purposes and policies of the Wiretap Act." *Id*. at 1081.

II. Plaintiff's Ohio And Cicvil Claims Were Wrongfully Terminated

A. Plaintiff's Claim Against Awareness For Intercepting and Disseminating His Electronic Communications Satisfies The Elements Of Ohio's Wiretap Act.

Under Ohio law, an aggrieved person may bring an action for damages against a company for either (1) intercepting an "electronic communication" or (2) for disclosing the contents of an electronic communication, when the company would have "reason to know" the contents were illegally intercepted. O.R.C. §§ 2933.51–.52; *Nix*, 160 F.3d at 348–50. "[T]he trier of fact may rely on circumstantial evidence to prove 'reason to know.' " *Nix*, 160 F.3d at 349; *accord United States v. Wuliger*, 981 F.2d 1497, 1502 (6th Cir. 1992) (concluding that "reason to know" requires that a seller have her eyes open "to the objective realities of the sale").

As under federal law, Ohio laws are implicated because Plaintiff claimed- and Tech never disputed- that Awareness used the acquired data by maintaining it online, processing user "alert words," and disclosing to its clients the contents of intercepted communications. (

Ohio recognizes the tort of invasion of privacy when a plaintiff's private activities are intruded upon "in such a manner as to outrage . . . a person of ordinary sensibilities." *Sustin v. Fee*, 431 N.E.2d 992, 993–94 (Ohio 1982); *Housh v. Peth*, 133 N.E.2d 340, 343–44 (Ohio 1956). While Ohio requires more than mere indignities to satisfy the tort, *Yeager v. Local Union 20, Teamsters, Chauffeurs, Warehousemen & Helpers of America*, 453 N.E.2d 666, 671–72 (Ohio 1983) *abrogated on other grounds by Welling*, 866 N.E.2d at 1059, Ohio law does not set an unattainable bar; repeated efforts to obtain information by a party, even without malice, can suffice. *Welling*, 866 N.E.2d at 1057–59; *see Charvat v. NMP, LLC*, 656 F.3d 440, 452–54 (6th Cir. 2011) (applying Ohio law to conclude that thirty-three unsolicited telephone calls over a three-month period constituted an invasion of privacy given the strong interests preserving the sanctity of one's home).

B. Claim For Intercepting and Disseminating His Electronic Communications Satisfies The Elements For Intriusion to Seclusion

The most commonly pursued claim is for intrusion. *See, e.g.*, *Housh*, 133 N.E.2d at 343. To succeed, a plaintiff must allege that a wrongful intrusion into a private place occurred in a manner offensive to a reasonable person. *Id.* at 344; *see also Steffen v. Gen. Tel. Co.*, 395 N.E.2d 1346, 1349 (Ohio Ct. App. 1978). "The intrusion alone is enough so long as it goes to a truly private matter and is of anature to cause mental suffering or humiliation to a person of ordinary sensibilities." *Steffen*, 395 N.E.2d at 1349.

In weighing offensiveness, courts evaluate the "totality of the circumstances," which encompasses the nature of the interference, the individual's private rights, and the public's interest in the intrusion. *Kohler v. City of Wapakoneta*, 381 F. Supp. 2d 692, 703–04 (N.D. Ohio 2005) (citing *Housh*, 133 N.E.2d at 343). But when determining an intrusion's wrongfulness,

the court need only evaluate how the intrusion was made to determine if it exceeded the bounds of reasonable behavior. *See Kohler*, 381 F. Supp. 2d at 704; *Strutner v. Dispatch Printing Co.*, 442 N.E.2d 129, 132 (Ohio Ct. App. 1982) ("'Wrongful' does not require that the intrusion itself be wrongful in the sense that there is no right to make any intrusion. Rather, 'wrongful' may relate to the manner of the making of the intrusion . . . ."). This is because the injury is not rooted in the intruder's procuring information, but rather in protecting "the person's interest in solitude or seclusion" from "intentional interference." *Kohler*, 381 F. Supp. 2d at 704.

Intercepting private communications such as emails and IMs constitutes an invasion of privacy under Ohio law. *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 760–61 (N.D. Ohio 2013). The plaintiff in *Lazette* claimed invasion of privacy by a co-worker who accessed her private email account without permission. *Id*. The court found that the plaintiff reasonably expected that no one would access her email account, "particularly in light of her unawareness of [the defendant's] ability to do so." *Id*. The court found the plaintiff's emails "highly personal and private" and that a reasonable jury could find the defendant's reading of "tens of thousands of such private communications . . . highly offensive." *Id*.

Invasion of privacy occurred by Awareness, because Plaintiff's private communications constituting "thousands" of "AOL instant messages" and emails over more than a month Awareness without his knowledge or consent. These repeated interceptions (thousands of which are in evidence as intercepted instant messages, each of which is considered an intercept) exceeded the mere double-digit volume of communications found to be

intrusive in *Charvat*.[16] private but for Awareness's intentional interception of his communications.

C. The MC Erred In Finding Plaintiff's Expectations Of Privacy under Ohio Law Was Inherently Diminished Due To A Lowered Expectation Of Privacy For The Married .Victim In The Case.

The majority of courts that have examined the issue of intra-spousal privacy have held that spouses are no different than other individuals; spouses do not forfeit through marriage their expectation of privacy, even from one another. The cited cases apparently favored and endorsed by the MC are outdated and backwards looking cases that are in the minority that have all depended on *the absolute worst* circuit court decision in our lifetime; one so bad it's a somewhat of a laughing stock among the circuit courts. (see *Simpson* below).

Moreover, discussions or concerns about the ownership of the computer used in Ohio are of no consequence. First, even if ownership of the computer were relevant, it is a disputed fact that is for a trier of fact to decide; the jury. Nonetheless, contrary to the MC's assertion, WebWatcher was installed on a computer purchased during the marriage and is considered co-owned in the state of Ohio. Second, neither the federal Wiretap Act nor the Ohio statute provides an ownership exception to liability. See 18 U.S.C. § 2511(2)(d); Ohio Rev. Code Ann. § 2933.52(B)(4). The only stated exceptions are for interceptions made by a party to the communication or when such a party has consented to the interception. Id. Ohio law defines marital property to include "[a]ll real and personal property. . . owned by either or both of the spouses . . . that was acquired by either or both of the spouses during the marriage." Ohio Rev.

[16] Moreover, Tech's "monitoring" of "anything typed in real time" which Tech never actually denied (they just insist it is not contemporaneous, but it is still considered "real time" if only for marketing purposes) along with the storage and processing of these communications served no public aim; indeed, its purpose was to disturb Plaintiff's private rights. Such monitoring was as invasive as the reading of personal emails in Lazette if not worse, as Plaintiff could never have consented to (or had reason to believe) his communications were being monitored. To Awareness, Plaintiff may be mere collateral damage of the wrongful acts of others; yet his private life would have remained scarred.

Code Ann. § 3105.171(A)(3)(a)(i). Plaintiff can prove at trial that the computer was definitely purchased within two years of the start of the divorce proceedings. Catherine Zang would have attested to that at trial. Moreover, she kept the computer after the divorce because Mr. Zang barely knew how to turn the thing on, and needed his computer savvy sister to install Webwatcher for him. That is also in evidence within the records of this case (As noted by the MC in RRR on page 24, as well as in prior exhibits containing Joseph Zang's testimony) as well as the divorce case which preceded this one. during "the period of time from the date of the marriage through the date of the final hearing in an action for divorce or in an action for legal separation," it was marital property to which both spouses had an equal claim of ownership. Ohio Rev. Code Ann. § 3105.171(A)(2)(a). Again, this is a question of fact for a jury to decide and yet another issue where Plaintiff has shown that there do remains questions of fact in this case. This Court recognizes an expectation of privacy in emails sent through commercial internet providers. *United States v. Warshak,* 631 F.3d 266, 286, 288 (6th Cir. 2010). Plaintiff was "surely entitled to assume that his conversation [was] not being intercepted" without his consent regardless of who owned the computer used by the other party to his conversation. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (discussing expectation of privacy in context of a public telephone booth and noting that "[t]he point is not that the booth is 'accessible to the public' at other times . . . but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable"). A reasonable jury will easily find that Awareness illegally invaded Plaintiff's privacy. Intercepting electronic communications, such as email and IMs, constitutes an invasion of privacy under Ohio law. *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 760–61 (N.D. Ohio 2013). Here, Awareness has submitted to Plaintiff during discovery evidence hundreds if not thousands of intercepted Instant Messages revealing constant automatic surreptitious surveillance for at least a month and a half.[17] They were also submitted to Catherine Zang in the previously attached case. Awareness intercepted his "private communications" including "thousands" of emails and AOL IMs. Awareness knew or should have known its product would be used for just such invasions of

[17] Given the illegal nature of the stolen communications, plaintiff could not admit them into evidence or submit them in a public filling.

privacy. Tech's argument that it had no viable link to the other defendants who allegedly disclosed his private communications" ignores the obvious. Had Awareness not intercepted Plaintiff's private communications and disclosed them to its customers, no other defendant could have accessed them. In other words, the initial intercepts and disclosures were made by Awareness; the other defendants' use of the communications was derivative.

D. Tech is Not Entitled to Judgment on Plaintiff's §2512 Claim Because Tech's Acquisition of Plaintiff's Communications State Causes Of Action Under The Different Standards Of Ohio Law.

The MC states that Awareness remains entitled to judgment as a matter of law on Plaintiff's alternate theories that the Defendant "intentionally disclose[d]…the contents of any…electronic communication, knowing or having reason to know that the information was obtained through the interception of …electronic communication," or that Defendant "use[d]" the contents of information "obtained through the interception of…electronic communication." Id. However, Awareness "used" Plaintiff's communications by disclosing them, having reason to know that the contents were obtained by illegal interception. Ohio Rev. Code § 2933.52(A)(3) (2015). Tech violated Ohio Wiretap Act and invasion of privacy claims because (contrary to the Magistrate Judge's assertion) allegations of personal knowledge or an agreement are not needed for these causes of action. (R. 109, R.&R., PageID # 764.)

The MC also confused the intent requirement in the ECPA. Tech touts its software as a means to "monitor a cheating spouse's computer without bringing undue attention." Indeed, the entire business model is based on WebWatcher's ability to surreptitiously intercept electronic communications. Operating through or on a third party device doe snot relieve a software designer of liability for intentionally intercepting communications. Like the software developer in *In re Carrier IQ*, Tech's conduct (developing and marketing WebWatcher) and the results achieved (intercepting Plaintiff's communications and routing them to its servers for storage) indicate intent.

In re Pharmatrak Inc. Privacy Litigation, 329 F.3d 9, 22-23 (1st Cir. 2003). In *In re Pharmatrak, Inc. Privacy Litigation*, the First Circuit remanded the case to the district court for a determination of whether the defendant company intentionally violated 25 U.S.C. 2511(1)(a) of the ECPA. 329 F.3d 9, 22-23 (1st Cir. 2003). In discussing the meaning of the term "intentional" in the ECPA and in its legislative history, the First Circuit noted: Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. An act is not intentional if it is the product of inadvertence or mistake. There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct. 329 F.3d at 23. On remand, the district court discussed whether a web-monitoring corporation's gathering of certain personal information of internet users for use by pharmaceutical companies was intentional in violation of 25 U.S.C. 2511(a)(1) of the ECPA.

E. Licensing Agreement

The MC went on at length about the licensing agreement. (Doc.# 225 at p. 23-26). The MC seemed to believe that Tech's agreement showed the company had attempted to "protect the rights of victims similar to the Plaintiff, requiring purchasers to accept its licensing terms prior to being allowed to install its software." *Id*. At 26. The MC then again employed its typical use of questionable case law and selective interpretation by using the case of *Hayes v. SpectorSoft Corp.,* 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009) to support its findings, while ignoring the huge differences between the facts of these cases. Moreover, the *Hayes* decision shows logical and internally inconsistency throughout the report. *Hayes* at *5–6 (E.D. Tenn.

Nov. 3, 2009). In *Hayes*, the court rested its analysis on the terms of the software's license agreement, which required customers to agree to "inform anyone who [sic] you may record that their Internet and PC activity is subject to being recorded and archived." Id. at *3. Based on this, the court found that the developer would be "unaware" that a person was "breaching the terms of its licensing agreement." Id. at *8. But the court dismissed an argument that the software should notify those being monitored because "[s]uch notices would reduce the efficacy of the legitimate uses for [the] software, such as employee and parental monitoring." Id. at *8. The court said in one breath that the designer reasonably expected customers to inform subjects that they were being monitored and, in the next, that alerting subjects would "reduce the efficacy" of the software. This obvious inconsistency highlights the disingenuous nature of finding that a licensing agreement trumps the software's design in analyzing intent. Nothing in the record suggests that Tech expected its customers to inform those monitored that WebWatcher would surveil their communications. Nor would that expectation be reasonable given Tech's emphasis on WebWatcher's invisibility and design to "catch cheaters."

Further, concerning Ohio's product liability law, Plaintiff alleged Awareness owed the general public a duty to manufacture and maintain a safer product of intercept,[18] and its intentional failure to do so released a device of intercept into the stream of commerce, which device was the direct cause of Plaintiff's injury and loss. Web Watcher is certainly a "product" under the Wiretap Act. A reasonable jury would find that WebWatcher was unreasonably dangerous at the time it left the manufacturer, in that Awareness had not incorporated any reasonable safety measures into its design, and its advertising for illegal use left rendered its

[18] While generally, a manufacturer of spyware software owes no duty to avoid emotional injury to the victim of the misuse of that software in violation of the software's licensing agreement, when a manufacturer markets a product for the specific purpose that caused the injury, it should be barred from later claiming that it owed no duty to those harmed by the use of the product in accordance to its marketing scheme.

product particularly vulnerable–indeed *likely*–to be abused by the users its marketing campaign specifically targeted.

Awareness' blatant failure to mitigate the easily foreseeable misuse of its product, particularly in light of its active advertising for such use, enables both the end user and the corporation to continue to freely prey on our constitutionally protected communications. Reasonable steps to protect the public from illegal intercept of our private communications have never been taken by Awareness as such precautions would counter their aggressive business model—on that primarily relies on such thievery in order to remain atop the spyware industry in sales and monthly memberships. Moreover, Awareness' aggressive advertisements represent intentional misrepresentations strongly implying that the surreptitious recording of spouses or associates is legal, for if not, could they be *openly advertising* Web Watcher for such use? Coupled with Awareness' failure to incorporate reasonable, cheap and effective safety functions—such as the inclusion of pop-up banners informing users that their private conversations are being surreptitiously monitored—Awareness illegal business model continues to evidence a bold-faced effrontery for the laws of this land, and the constitutional protections afforded our private communications. Even to this day, Awareness continues to operate as *the absolute worst* offender within an already insidious and near monolithic world-wide corporate mechanism of private intercept that Congress never imagined would be allowed to exist due to the protections it intended in its drafting and amending of the Act. Thus, little imagination or further reasoning is needed for this Circuit to find that Awareness' role in the present action represents a gross and actionable negligence of the highest degree, and one it *must* be held accountable for in this action, if not under the Wiretap Act, then under suitable common or state provided laws. *Gootee v. Colt Industries, Inc.*, 712 F.2d 1057 (6th Cir. 1983)((reversing lower

court's judgment of no cause of action, finding that there was sufficient evidence to send misrepresentation and negligence in design to the jury. Additionally, finding that in product liability action grounded in negligence, a manufacturer could be held liable if it failed to guard against dangers posed by foreseeable misuse).

III. Plain Language Aside, The Legislative History And Policy Considerations Also Support Interpreting The Act To Equally Protect Electronic Communications In Transit And Those In Storage.

A. Congress did not intend a contemporaneous requirement

Congress did not intend a contemporaneous requirement for at least three primary reasons, as follows; (1) because Congress' goal was to expand the protection of electronic communications not limit protections, and (2) a congressional report that Congress relied on explicitly stated that emails could be intercepted in storage after transmission, and finally, (3) Interpreting the Wiretap Act without reading in a contemporaneous element was Congress' intent when it wrote the Wiretap Act and then later expanded it with its later passing of the The Electronic Communications Privacy Act of 1985 (ECPA).

The ECPA was passed in the mid-1980s because the advent of electronic communications at the beginning of the decade (principally email) suggested to many that the Wiretap Act needed revision. *Councilman*, 418 F.3d 67at p.*76. Thus the ECPA was introduced to amend the Act to incorporate electronic communications—largely emails (and later instant messaging). *Id.* Shortly after the bill was introduced, the Congressional Office of Technology Assessment released a study of the privacy implications of electronic surveillance *Id.*;[19] The

[19] See Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties, available at http://www.wws.princeton.edu/ota/disk2/1985/8509_n.html (Oct.1985) ("Report").

Report listed five stages at which an email could be intercepted. *Id.* (emphasis added). The stages at which interception could occur included "in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes." *Id.* at 48. The Report went on to note that existing law offers little protection and emphasized that "interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties." *Id.* at 48, 50 (emphasis added). Congress passed the bill based on this study and against the Department of Justice's wishes, which wanted to give less protection to electronic communications. *Councilman*, 418 F.3d at 76-77.

Congress did not intend a contemporaneous requirement because the congressional report Congress relied on explicitly stated that emails could be intercepted in storage after transmission and because Congress' goal was to expand the protection of electronic communications. A contemporaneous requirement would nearly remove emails from the purview of the Act because emails are actually in flight for only a short period of time. There is only a narrow window during which a contemporaneous email interception may occur—the seconds or milliseconds before which a newly composed message is saved to a temporary location following a send command. *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003). Unless an email is intercepted in that split second, Defendants' reading of the Act effectively makes it impossible for email interceptions to violate the act. *Id.* Furthermore, the Act itself defines electronic storage to include any temporary or intermediate storage of an electronic communication. *Id.* § 2510(17). Because emails are consistently in intermediate storage as they travel through the internet, and because Congress plainly stated even intermediate storage counts as storage, Defendants'

contemporaneous argument would effectively remove all emails from the purview of the Act. This is an especially absurd conclusion as one of the amendment's primary goals was the protection of emails. Congress intended the broad definition of electronic storage to offer broad protection to stored communications, not to exclude them entirely from the purview of the Act. *Councilman*, 418 F.3d at 77-78 (Congress sought to ensure communications in pre- and post-transmission storage were protected. Congress, responding to the Report's concerns, sought to ensure that messages "stored in a user's mailbox are protected from unauthorized access"). This is why *Councilman* and its progeny resort to legal acrobatics to piece together a contorted reading under which there is a contemporaneous requirement but one that does not always apply to all communications in storage. *Councilman*, 418 F.3d at 79. The more straightforward approach is consistent with Congress's intent and the Act's plain language—the Act does not distinguish between electronic communications in storage and in transit.

B. The modern trend in case law and Congress' intent require construing the Wiretap Act without a contemporaneous requirement

The recent trend in case law is that a distinction between electronic communications in transit and in storage is unrealistic and problematic. The recent trend, to eliminate the storage/transit dichotomy, applies the better reasoned, more practical approach than the string of outdated cases relied on in the RRR. In *Potter*, a more recent case than those cited by Defendants, the Southern District of Ohio presented a more reasonable reading of the Wiretap Act when it found the Act did not require a contemporaneous element. *Potter v. Havlicek*, 2007 U.S. Dist. LEXIS 10677, *19 (S.D. Oh. Feb. 14, 2007). In ruling on the merits of the case, the court refused to follow other circuits' "hyper-technical application of the contemporaneous

requirement" in the Wiretap Act and instead found that the emails did not need to be intercepted contemporaneously. *Id.* at *18.

The *Potter* court found merit in Judge Reinhardt's concurring and dissenting opinion in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 886 (9th Cir. 2002). *Id.* at 18. The *Potter* court also found merit in *Councilman*, 418 F.3d 67. There, the First Circuit determined that the contemporaneous requirement, which had been inserted by earlier courts, was not a requirement under a proper interpretation of the Wiretap Act and upheld Mr. Councilman's conviction. *Id.* at 78-9. *Councilman* represents the more logical, well-reasoned, and proper analysis of the "contemporaneous" requirement than *Councilman* was also an *en banc* opinion of the First Circuit. In *Councilman*, the First Circuit reversed the lower court's dismissal of Councilman's indictment because the lower court improperly relied on the second *Konop* decision to read a contemporaneous requirement into the act. *Id.* at 71. Councilman was indicted for directing its server to intercept and copy email messages passing through its servers from Amazon.com to Councilman's customers. *Id.* at 70. Councilman's interception occurred only while the e-mails were in storage on Councilman's computer. *Id.* at 71. The court in *Councilman* analyzed the Wiretap's plain language and legislative history and, for the reasons stated supra, found that Congress amended the Act to offer greater protection to emails located in storage—not to exclude them from the Act's protection. *Id.* at 72-79. There can be no contemporaneous requirement because Congress drafted the Act to protect emails in storage.[20] This Court should also find the *Hall* opinion instructive, in which the Second Circuit rejected the argument that

[20] Although the First Circuit in Blumofe did not need to rule on the existence of a contemporaneous requirement, it noted that it shares the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and World Wide Web in a case involving purported interceptions of online communications. Blumofe v. Pharmatrak, Inc. (In re Pharmatrak, Inc. Privacy Litig.), 329 F.3d 9, 21 (1st Cir. 2003) (Citation Omitted). The court noted: "In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems." Id

"communication over the Internet can only be electronic communication while it is in transit, not while it is in electronic storage." *Hall v. EarchLink Network, Inc.,* 396 F.3d 500, 503 n.1 (2d Cir. 2005).

C. Tech Should Not Be Granted Judgment On The Section 2511 Claims Because As This Same Court Once Noted, Other Courts Operating Under The Contemporaneous Standard Have Found The Timing of Intercepted Communications To Be "Contemporaneous Under Any Standard"

From pages eight to eighteen, the MC's Report discusses in depth why it recommends Tech should be granted summary judgment on Plaintiff's section 2511 claims. Interestingly, the MC now advocates the exact opposite of what this same Court argued in its RR back in 2013 (Doc.#109) The turnaround in philosophy is not explained by the Sixth Circuit's recent adoption of the contemporaneous standard since it could have argued the same points within the boundaries of the contemporaneous standard as have other district courts and Circuit Courts. Regardless, the MC has applied an overly stringent and improper interpretation to the terms within the contemporaneous standard. In the alternative, Plaintiff believes the Sixth Circuit should adopt the broader interpretations of the First and Seventh Circuit because, among other things, the Act/ ECPA's anti-interception provision does not in any way stipulate that "interception" of electronic communications must be contemporaneous with their transmission While subsequent circuit court case law, such as *Fraser v. Nationwide Mutual Insurance Co*. (352 F.3d 107, 113 [3rd Cir. 2003]), "has held that an 'intercept' under the ECPA must occur contemporaneously with transmission." However, other circuits have taken a more advanced approach, having either formally or informally adopted a broader approach to the intercept question that plaintiff believes is much more technically sound and constitutionally proper. In

most of those cases the courts did not necessarily deviate or reject this Circuit's recently adopted contemporaneous standard – rather they simply recognized the full set and type of data meant to be protected by the Wiretap Act. In truth, a vast re-thinking of the contemporaneous standard –if not its rejection entirely– really *should be* explored in this case in order to right the many wrongs created by the judicial system in its decades-long "emasculation" of the Wiretap Act.[21] Nonetheless, a mere adjustment or tweak of the terms is all that is necessitated for now to get this case its proper day in court; a necessary and critical adjustment that will also protect hundreds of thousands of future victims (mostly female) whose ongoing abuse by their spouses is exponentially increased buy their spouses use of this maliciously designed and marketed spyware. In fact, aiding the already battered and abused Act was the original reason Plaintiff brought about this lawsuit in the first place back in 2011.

D. The Wiretap Act's plain language makes no distinction between electronic communications in transit and those in electronic storage.

Nowhere in the Federal Wiretap Act does it state that an electronic communication cannot be intercepted while it is in storage. In fact, the Wiretap Act never mentions "electronic storage" in any of its relevant provisions. Tech and the MC would have this Court believe that the Act creates a dichotomy between electronic communications in transit and electronic communications in storage and that the Act only protects the former from interception. This is plainly untrue. The Act treats electronic communications in transit and in storage identically. The plain language of the Wiretap Act never states that electronic communications can only be intercepted simultaneously with their transmission. The Act applies to "wire communications,"

[21] As just one example, in *Potter v. Havlicek*, 2007 U.S. Dist. LEXIS 19 10677 *11, Judge Rose opposed "a hyper-technical application of the contemporaneous requirement emasculating the ECPA."

"oral communications," and "electronic communications"; each of these three communications are treated differently under the Act. 18 USC § 2511(1)(a) (LEXIS 2015). The Act's own language limits wire communications and oral communications to contemporaneous interceptions but refuses to extend such an interpretation to electronic communications.

E. The Plain Language of the Wiretap Act Does Not Require A Contemporaneous Requirement and Congress Defines Intercept To Include Acquisitions, Which Need Not Be Contemporaneous Under Any Standard.

By the Act's plain language, canons of construction, and the legislative history of the Act, it is obvious that Congress did not intend for electronic communications in storage to fall beyond the purview of the Act, and that to do so would produce an absurd result in the interpretation of the Acts protections. Such an approach is supported by the reasoning used in *Councilman*, as follows.

> The district court seemed to agree with one predicate of the Government's argument when it acknowledged that "technology has, to some extent, overtaken language" and that "[t]raveling the Internet, electronic communications are often— perhaps constantly both `in transit' and `in storage' simultaneously." *Councilman*, 245 F. Supp. 2d at 321. This apt observation should have prompted a different legal conclusion.
>
> All digital transmissions must be stored in RAM or on hard drives while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an e-mail message must store those packets in memory while it reads their addresses… Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.

This Court should find the more recent string of cases that apply the Act to electronic communications in storage more persuasive than those of the outdated cases relied upon by the circuits that adopted the narrower interpretation; cases that rely on a version of the Act that has since been amended.

Unlike with wire communications, Congress did not restrict electronic communications to communications in flight. Congress chose to omit wire communication's requirement of

"between the point of origin and the point of reception" from the definition of electronic communications. *Id.* § 2510(12). Congress also chose to replace wire communication's "aural transfer," which requires the transfer to be "at any point between and including the point of origin and the point of reception," with electronic communication's "any transfer." *Id.* § 2510(18); § 2510(12)(emphasis added). To ensure that there is no confusion, Congress specifically stated that electronic communications exclude wire and oral communications. *Id.* § 2510(12) If Congress intended to include a contemporaneous requirement as to electronic communications, it would have included the contemporaneous language it included in wire communication and aural transfer. Where Congress includes particular language in one section of a statute but omits it in another section of the Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion. *Russello v. United States*, 46 U.S. 16, 23 (1983). Furthermore, Congress specifically enumerated four exceptions to electronic communications, one of which had to do with a certain type of electronically stored information. *Id.* § 2510(12). If Congress wanted to exclude all stored electronic communication from the Wiretap Act, it would have done so here. Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied in the absence of evidence of a contrary legislative intent. *TRW v. Andrews*, 534 U.S. 19, 28 (2001); *Councilman,* 418 F.3d 67, 75 (rejecting Defendant's argument that Congress intended to exclude stored electronic information from electronic communications because if Congress wanted to do so it would have included it as a numerated exception to electronic communications).[22]

[22] In fact, the only purported support whatsoever contained within the four corners of the Act is the ordinary usage meaning of intercept, which may suffice in football but is useless to address the nuances of an email's transfer throughout the web. *Szymuszkiewicz,* 622 F.3d 701, 705.. However, Congress chose to define intercept instead of relying on its ordinary usage meaning by defining it as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4) (emphasis added). If Congress wished, it easily could have added its contemporaneous requirement in wire communications and aural transfer into its definition of intercept. Wesley College v. Pitts, 974 F. Supp. 375, 386 (D. Del. 1997) (agreeing that Congress could have added the language if it intended a contemporaneous requirement, but rejecting that argument in favor of an argument based on a textual contradiction,

IV. Questions of Fact remain that Should be ruled on by a Jury

A. Question concerning the type of communications acquired

A good analogy as to the difference between an email and instant messages is a river and a lake. An email is being sent to a stagnant lake with a defined area. Instant messages travel more like a river. Information packets are constantly flowing in and out of the computer of both parties. An email is more of a one-time packet (even if it does get split into different packets, it is one overall packet) whereas Instant messages are an endless flowing stream of packets. Thus, while the spyware is tracking communications input by the end-user onto his or her own computer, the time between the end-user's input and the actual transmission of the bits of data to the other communicant is so short, on the order of milliseconds, that the communication begins contemporaneously with the end-user's input. The courts have not yet credited this argument. However, Plaintiff hopes this will be the first. if they did, then a majority of spyware programs installed without actual consent could be found to violate the Wiretap Act, and consumers could have another cause of action against spyware proliferators. Therefore, because WebWatcher is an extension of Tech during the intercepts, through an invisible ineffable connection between them during the period of active intercepts, anything Webwatcher acquires – even if on the RAM of the computer and not on internet lines of communications – can be seen as being copied while the information is still in transmission or moving on a system that affects lines of commerce. In

which, as noted below, Congress has since corrected). Not only did Congress not apply its contemporaneous language from terms defined before and after intercept, but Congress added the key language of or other acquisition to ensure intercept need not be contemporaneous. Id. § 2510(4). Acquisition's plain meaning is to acquire or gain—contemporaneous is not an element of acquisition, regardless of the usage. Congress did not intend a contemporaneous requirement because it defines intercept to include the acquisition of emails.

short, Webwatcher becomes an erstwhile extension of a service provider reaching into the desktop but connected to the internet at the same time. Therefore, given that relationship, the communications is never seen as truly stopping from being in transmission when instant messages are involved. And those are the main kind of communications involved in this case.

B. Question concerning the intended endpoint of a communication

In its previous Report from 2013 (Doc #109), the MC properly noted the following; "The courts adopting this holding have reasoned that the term "intercept" as defined in the Wiretap Act requires interception of the communication either before it reaches the intended recipient, or 'contemporaneous with transmission' – but not after it reaches that destination when presumably, the data is placed in electronic storage." See, e.g., *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003). The Appellate Court also noted the relationship between the "contemporaneous" standard and when the message reaches its final intended place, essentially saying the same thing. *See Luis v. Zang*, 833 F. 3d 619, 627 (6th Cir. 2016). A theme emerges; once concerning motion and lack thereof of a communication. While this may well be true, the MC was exploring the facts of this case in the context of cases that mostly dealt with emails. However, this case has dealt mostly with Instant Messages. An email travels through the internet, it goes into the recipient's email account residing on a server somewhere (usually Google or some other service, but mostly AOL in this case). From there the recipient requests the service to send them the copy. Until this point, WebWatcher, which resides on the recipient's computer only, has done nothing but perhaps copy the screen showing receipt of a new email which only contains mostly harmless header information, and not much private content of the actual message (though that in itself can be considered an acquisition of private messages). However, that message has not yet technically arrived at the recipient's computer. But once they click on the

email, it is then either opened up immediately or downloaded to their computer. It is then that WebWatcher strikes. The communications stopped traveling through the internet and go through to the computer's ram and then "saved" somewhere on the computer's drive. However, WebWatcher copies it before it gets to that final intended destination when the email goes straight to the persons computer. It does not do so when the email goes to rest on, say, Gmail's server or some other service. By the time the message gets to the recipient, that message has already been stored on gmail's server. With an instant message, the final intended destination is a different thing altogether, and it is not one that is easily answered. For what is the final destination of an instant message? What storage platform is involved? The RAM? Is that the final intended destination as a hard drive is for an email? Unlikely. As an instant message's signal leaves the internet and goers into the computer, the message can be seen to remain in "transmission" to its intended destination or endpoint where it "comes to rest" only when it reaches the recipient's screen. So that RAM can not be considered its final destination or resting place. This question has been visited by previous cases, and this is a question that should be explored herein. Although the message has not really "come to rest" nor reached its "final destination," (nor even truly been placed in "electronic storage" due to the fact that RAM is not really considered "storage" but "memory" - even if it can do both things at once) it *is* still technically moving from RAM, where it then goes to VRAM, then the screen. This has been also been explored in a few cases where the question of whether or not a computer is an Electronic communications service" ("ECS") has played a central role. *See Chance v. Avenue A, Inc.,*165 F.Supp.2d 1153, 1161 (W.D.Wash.2001) (leaving open the possibility that personal computing devices are "facilities" under the SCA); *United States v. Park,* No. CR 05-375 SI, 2007 WL 1521573 at *8 (N.D.Cal. May 23, 2007) (explaining that the line between cell phones and

computers has blurred because "[individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant message"). While these cases have involved the SCA, the Wiretap Act can also be implicated.[23]

And that question can certainly play a role herein. However, another question should perhaps be explored in this context. When there is an intended or destined "place of rest" for an email – for example a storage location such as a person's hard drive or a server location from Gmail or other service provider – we can think of an email being sent to a place of rest, or storage or a "bed" if you will. In that ciontext, the previous definitions make sense. then the email can get to its intended destination where it then stops for all eternity- or until the recipient erases it from the drive. However, it is doing so in the computer itself, and not through internet lines. Right or wrong (wrong) most courts–but not all- interpreted the ECPA to require that the messages must be intercepted while traveling on the internet lines, although even with those courts, some say while the message is traveling on a system that affects interstate commerce."

[23] Significantly, the SCA it is not limited to unlawful access to a computer or facility alone. Instead, it also prohibits such access to a *network* without authorization. Therein lies a mildly complicated concept relevant to Appellant's SCA claims. At the time of the alleged violations of the Act by Tech, Appellant used various Internet Service Providers ('ISPs'), such as America Online ('AOL"), Yahoo, and Gmail to both send and receive emails and instant messages. All of the above ISPs are considered ECS as defined in the SCA. The majority of the relevant communications rerouted by Web Watcher onto Tech' private servers were obtained somewhere within a temporary amalgam of purpose created within cyberspace. This practically indefinable union of personal devices and infrastructure represented a communications tunnel or perhaps cubicle—practically a high tech virtual phone booth—carrying and temporarily hosting constitutionally protected communications. The tunnel is formed by a technically complex interaction between 1) Appellant's personal computer, 2) the privately owned servers and software of AOL,[23] 3) the Internet's publically accessible infrastructure, and 4) the computer of the intended recipient of Appellant's communications, Ms. Zang, who Appellant believes also primarily depended on those three ISP's for her Internet-based electronic communications. In addition to intercepting every single message both to and from Ms. Zang's computer, Web Watcher also recorded all of her browsing history and took snapshots of websites visited, as well as snapshots of instant message sessions, along with the intercept of those messages themselves.

That distinction is critical because a computer is considered a system that affects interstate commerce, and that is a critical component of a "contemporaneous" intercept. Of course, that means it is virtually impossible to "intercept" under the ECPA. Regardless of the judicial system's long-standing assault[24] of the Acts intended protections, those include emails; something not as popular as it once was because of texting and instant messaging. With email there is a final resting point, and storage of one type or another is its natural destiny, if you will. But not so with instant messages. They live and die with every session, not saved anywhere, unless a spy program is doing so. Their intended natural endpoint is to be acknowledged and responded to. Not storage of any kind. So until there is a response, has their been a communication in a live setting? It is perhaps a “tree falls in a forest” type of question, but it is a question that should be asked and explored. But with Instant Messages, there is no “final destination” since the Instant messages disappear once the recipient is done with the conversation. In fact unlike a hard drive or server somewhere, an instant message’s “final destination” is the recipient’s screen, and in fact it may go further and find that an instant message’s intended final destination is it’s intended recipient’s acknowledgement and response, since instant messages are more “live” than paperweight type of communications.; as are emails. So the distinctions between emails and instant messages extend into a metaphysical arena which extends beyond questions of law, and into questions more properly decided by a jury. or, but not the RAM. In fact, this should be the more technically and constitutionally correct posture to adapt. not the RAM. A jusy could find that a message still travelling to its intended natural destination where it will “rest” Unlike an email, the destination or endpoint is almost NEVER some hard drive on the recipient’s computer. This was never contested by Tech. Even then when

24

it was acquired in the RAM, the message had not stopped "traveling" since it needed to go to the VRAM, which then sends the signal displayed on the screen. There the message never moves again and thus, "resting" as noted above.

In this lower forum, Tech never once raised any doubt or concerns about the advertisements submitted as exhibits pointing towards their illegal and illicit advertising strategy. Tech did for the first time question them during appeals, wherein Plaintiff's representatives responded "Awareness cursorily disputes the validity of these exhibits for the first time on appeal …As a threshold matter, because Awareness did not challenge the validity of these exhibits below, it cannot do so on appeal." Awareness's implied arguments that these advertisements were not paid for or sponsored by Tech,[25] at most create questions of fact. Concerning Tech's previous affidavit, the Magistrate Judge correctly found that Mr. Miller's affidavit "is wholly silent regarding when WebWatcher forwards the recorded information to the secret account." (Doc.# 109 at *13) Again Plaintiff's representatives correctly replied, "Awareness did not object to this finding…. Accordingly, Awareness has waived its ability to challenge this finding on appeal."[26] Similarly in this lower forum, nothing Tech has submitted either to Plaintiff during discovery or to this Court clearly demonstrates that the actual functionalities of Web Watcher do not include a contemporaneous acquisition of electronic communications. This remains a question of fact. Moreover, as the MC noted in RR1, Plaintiff also alleged that Tech's "software did more than merely record keystrokes because it also saves and/or records entire IM conversations and other 'screen' data. A portion of the recorded data originated from Plaintiff,

[25] In appeals Tech also implied that the screenshots submitted within the exhibits were for a different spyware product called WebWatcher , or it was marketed by another company, or that it marketed WebWatcher differently when Mr. Zang purchased the product.

[26] Plaintiff is uncertain if the fact that Tech never objected or raised concerns about the exhibits within the first five years of this lawsuit, whether or not the issue is forever considered waived not only in that last appeal but in this lower forum, or if it is given new life upon reversal in appeals.

from a remote computer on which WebWatcher was (presumably) not installed. The affidavit submitted by the CEO confirms that much broader data than keystrokes is captured by the spyware at issue." *Id.* Thus, Tech's own CEO confirmed that – like most similar rootkit based software - Webwatcher also takes screenshots at certain intervals. That *confessed* (or at least strongly implied) functionality alone adds to the remaining questions in this case and that extra ability has often been the difference maker in past decisions as to whether or not an "interception" has occurred in a case. While Webwatcher was not on Plaintiff's computer and thus not taking screenshots of his computer screen, it was taking screenshots on Catherine's screen (or it had the ability to do so) which was also displaying Plaintiff's private conversations in the opened IMs. The ability to take screenshots alone qualifies the mechanism as being capable of producing prohibited interceptions even under an interpretation of the FWA that requires interceptions of electronic communications to be contemporaneous with transmission. *See ex. Shefts v. Petrakis*, No. 10-CV-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012) (finding that software that caused images of the plaintiff's email communications to be captured as they were being written and sent or received "contemporaneously captured Plaintiff's electronic communications within the meaning of the [FWA]"); *see also Potter*, 2007 WL 539534, at *6 (holding that "incoming emails subjected to the screen shot software" satisfy the FWA's definition of an interception of an electronic communication).[27] Moreover, any remaining dispute as to how WebWatcher works is a question of fact that the MC now seems to be feel has been resolved. With what evidence, Plaintiff remains unsure.

[27] Tech violated the FWA's prohibition on using unlawfully intercepted electronic communications when it summarized his private messages when they acquired them on their servers . See 18 U.S.C. § 2511(1)(d). Tech also violated the FWA's disclosure provision by having sent them via email to Joseph Zang. See 18 U.S.C. § 2511(1)(c*); see also Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009) (holding that 18 U.S.C. § 2511(1)(c) "protects against the dissemination of private communications that have been unlawfully intercepted").

Significantly, acquisition of AP's communications was never even *challenged* by Tech as there was plenty of evidence available to prove it had done so. Thus, arguing arguendo, even if *somehow* Tech was properly found innocent of liability for the *intercepts*,[28] Tech's "use" and "disclosure" clearly violated the Act because Tech did not challenge or address AP's claims (in the lower proceedings or in appeals concerning the following; 1) its advertising for illegal use was illegal, and 2) that they ***knew or should have known*** the illegal nature of the intercepts it was acquiring, using and disclosing. Therefore, Tech's summaries and deliveries given its undisputed ability (and/or duty) to know the illegal nature of the intercepts is a clear violation of 18 U.S.C §§2511(1)(c), (d).[29] This presents a problem for the SD because it never discussed whether Tech "knew or should have known" that the communications were being illegally acquired on its servers.[30]

Moreover, even the §2512 Wiretap Act claims can survive in some circumstances – at least in some courts.

Summary

The MC has awarded summary judgment against all of Plaintiff's claims Plaintiff on the MC's belief that Plaintiff's entire case lives and dies depending on whether an "intercept"

[28] An Intercept (§2511) was previously found to have occurred, and when it was the MC did not use any lax filing standards to get to that conclusion/recommendation. Rather it was a well reasoned and thought out exercise free of any standards outside of the right path to pursue in order to fulfill Congress; intentions when it authored the Act and then later updated it in the ECPA. The findings did not rely on any inferences or fact that are not present now. The messages were not acquired any quicker then. In its exploration, the MC even noted that whether it was instantaneous or within a blink of an eye, the proper standard was well reflected by the *Klumb* case. The MC dismissed thee case, but not because of this issue, which was ruled Plaintiff's way. Having been sent back, this ruling should have remained the same. Even if Tech acquires the communications from RAM, the millisecond's difference should not have caused such an improper and abrupt about-face by the MC. Tech's actual acquisition of Plaintiff's messages violation alone, with or without liability later attaching, would have been enough for the purposes of enabling standing to sue under §2512, as it was a violation of §2511. Most courts recognize a cause of action for §2512 when in the presence of any violations of §2511.

[29] Throughout these proceedings, Tech never one denied nor did it address AP's claims that it knew or should have known the illegal nature of the intercepts it was acquiring, using and disclosing.

[30] In the first half of this case, only by having *somewhere* explored or denied that Tech could not have known the illegality of the communications–an impossibility given Tech's advanced capabilities and infrastructure – could the SD have properly found that Tech's use and delivery did not violate §2511, thereby negating reach of remedies for violation of §2512. Instead, the MC looked towards other variables not considered relevant to liability under the Act.

occurred as written by the Wiretap Act and as is now interpreted by the Sixth Circuit. However, as interpreted by the First and Seventh Circuits, as well as various district courts. Interestingly, one of those court was within this circuit., and was heavily advocated by this Court in 2013; *Klumb v. Goan*, 884 F.Supp.2d 644, 647-48 (E.D.Tenn.2012). Moroever, the spyware used in that case, eBlaster, works virtually identical to the one used in this case both with emails and instant messages which it alone permanently captures and saves, since instant messages are not normally placed into permanent storage of any kind; rather they are only transported on temporary volatile storage and so this Court should adopt it while deciding on this Objection;

> eBlaster is a computer software program that can perform various spyware functions. It can record every keystroke made on the computer on which it is installed. It can also keep track of all websites visited and all applications used on that computer, and it can capture screenshots of instant messages and cached webpages. In addition, it can be directed to compile a report of this information at selected time intervals and send that report to a designated third party email address. Further, it can be directed to automatically forward copies of incoming email accessed on that computer to the third party email address. Each individual email is sent separately and independently from the eBlaster reports. eBlaster can also forward to this third-party email address copies of instant messages or "chat" messages as they are occurring.

–*Klumb*, 884 F.Supp.2d at pgs. *647-48

While instant messages may take a ride on RAM memory, they surely are not stored unless they are being copied by an automatic routing program as has been the case here. The notorious "contemporaneous standard" of intercept, while still less than satisfactory or even technically proper, nonetheless does minimally comply and can be seen to fulfill congressional intent when it authored the Wiretap Act and later updated it in the ECPA. However, as interpreted through the MC (and similar courts) the Sixth Circuit has has adopted a notorious loophole that has neutered the Wiretap Act for decades and that directly conflicts with two of this Circuit's biggest landmark privacy cases; *Jones* and *Warshak*. Of all the intercepting entities ever to appear in a US courtroom, Awareness Technologies represents the absolute worst. Not

only does it manufacture devices primarily meant for surreptitious copying of private information, it actively markets those devices for illegal use. And yet, despite this, the MC has written the company and that insidious industry a free pass to gather all our private information without any of us knowing until its too late. Tech's business is spying on private conversations through its software, WebWatcher which records everything that happens on a monitored computer: keystrokes, emails, instant messages, and more. All that WebWatcher records is kept on Tech's servers to be accessed by Tech's customers through Tech's Internet site. Plaintiff is a victim of Tech's spying. When one of Tech's customers bought and used WebWatcher to record his wife's Internet activity, Tech captured Plaintiff's communications as well. Plaintiff's claims under the federal Wiretap Act § 2511 and the Ohio Wiretap Act should not be dismissed because Tech intentionally intercepted his electronic communications. Previously in 2013, the Magistrate Judge correctly determined that WebWatcher intercepted Plaintiff's communications in its Report and recommendations (Doc. #109) but in its most recent Report due to the MC's inexplicable embrace of the absolute most narrow interpretation of the contemporaneous standard possible, leading to its improper conclusion that no intercept has occurred. The MC has either ignored altogether or misunderstood and misapplied the contemporaneous standard as has been applied by more recent Circuit court decisions. In fact, the MC could have allowed this case to continue onto trial, and yet remained well within the boundaries of the contemporaneous standard – just as one of its sister courts ruled in a ruling the MC found quite proper and fitting back in 2013.

As part of WebWatcher's design, Tech maintains an Internet-based platform to keep all of the communications WebWatcher records. Because WebWatcher has been certified by Tech as copying only from the RAM, it means it copies the information in milliseconds, which is

practically in real time then some seconds later sends the acquired information to Tech's servers for later access by its customers. Webwatcher is an extension of Tech during the period of intercepts and so when WebWatcher copied Plaintiff's incoming communications from the RAM, Tech's "agent" is the first entity to come into possession of Plaintiff's communications.Because communications is in the RAM before the intended recipient sees it on her screen –even if only milliseconds before - Tech "intercepts" within the ordinary meaning of "intercept," which is "to stop, seize, or interrupt in progress or course before arrival to its intended destination." *Id.* (quoting Webster's Ninth New Collegiate Dictionary 630 (1985)) When it copies the information is what's important, not when it is later sent to its servers. By design then, Tech is an informant, providing secretly intercepted information to WebWatcher's users for a fee. When its customers access that information is not relevant to Tech's interception. Second, through § 2520(a), the Wiretap Act provides a right of action for any violation of its provisions as long as a plaintiff falls into the narrow category of those who have suffered harm. Section 2520 operates in two parts. First, it requires that a plaintiff's communications have been intercepted, disclosed, or used in violation of the Act. A plaintiff so harmed may sue a defendant who engaged in violating the Act. Congress intentionally used broader language to define the class of defendants than it did in identifying proper plaintiffs. A manufacturer engages in the violation that caused the plaintiff's harm when there is a nexus between the manufacture of the product and the interception. Such a nexus exists when a manufacturer knows its device is primarily useful for intercepting communications and its product is used according to that design, which Tech surely must know. This Plaintiff has standing because his communications were intercepted and or acquired (acquisition was never challenged or disputed by Tech), used and delivered by a manufacturer that sold software that it knew was primarily useful for interception

(establishing a violation of § 2512). Plaintiff then connected these two—showing that Tech engaged in the violation that caused his harm—by pleading that the software Tech made was used to intercept or at least acquire, use and deliver his communications. Similar manufacturer liability has been recognized by the Supreme Court in the copyright context in *Metro-Goldwyn-Mayer Studios Inc., v. Grokster, Ltd.,* 545 U.S. 912 (2005), through reasoning that applies with equal force to the Wiretap Act. Cases that have found no private claim under § 2512 rely on language or logic rooted in superseded statutory language. As such, the cases finding no private right of action are unreliable. Even in courts that prohibit recovery for violations of §2512 alone, many allow liability "in the presence of intercept, use or delivery." *See e.g. See e.g. DirecTV, Inc. v.Moreno, 2003 WL 22927883 (D.N.J.)* at *2. Moreover, when statutes are written in the disjunctive, a party needs to prove only one of the factors to meet the statutory requirement. West's A.I.C. 35-33.5-5-4(a); *See also Dommer v. Dommer,* 829 N.E.2d 125 (Ind. Ct. App. 2005)(because the phrase "intercepted, disclosed, or used," was written in the disjunctive, plaintiff needed to allege that only one of those three violations occurred.). under common law invasion of privacy claim under Ohio law. Tech's repeated captures of his personal communications without his knowledge or consent intruded into the sanctity of his private life in a manner offensive to any reasonable person.

Conclusion

Forty years ago, this Circuit found that the federal Wiretap Act "establishes abroad prohibition on all private electronic surveillance and that a principal area of congressional concern was electronic surveillance for the purposes of marital litigation." *United States v. Jones,* 542 F.2d 661, 669 (6th Cir. 1976); see also *id.* At 667 (quoting Senate Report's statement of Wiretap Act's purpose as addressing the "tremendous scientific and technological developments

that have . . . made possible today the widespread use and abuse of electronic surveillance techniques"). This case presents *Jones's* logical extension to the Internet Age, at a time when companies like Tech intentionally intercepts and discloses private electronic communications for its commercial gain through WebWatcher, software it designed to help its customers catch a cheating spouse. The MC's ruling is obvious error and to uphold it would not only be a miscarriage of justice, but it will directly conflict with this Circuit's most notable landmark cases and its honorable record over privacy rights over the past half-century.

Dated: May 15, 2018

Respectfully Submitted

/s/ Javier Luis, Pro Se

jdluis65ohio@gmail.com

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Objection was filed electronically on May 15, 2018. Parties may access this document through that system.

/s/ Javier Luis, *Pro Se*